INSPECTOR GENERAL INSTRUCTION 4630.2, November 17, 1999

SUBJECT: Internet Policy

References: See Appendix A.

A. Purpose. This Instruction updates the Office of the Inspector General, Department of Defense (OIG, DoD), policy on appropriate access to and use of the Internet. It also advises OIG employees of their rights and responsibilities for accessing and using the Internet.

B. Cancellation. This Instruction supersedes IGDINST 4630.2, *Internet Policy*, August 1, 1997.

C. Applicability and Scope. This Instruction applies to the Offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; Director, Intelligence Review and the Office of the General Counsel (Inspector General), which is provided support by the OIG. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

D. Definitions. See Appendix B.

E. Policy

1. The OIG shall not create, send or receive classified or Sensitive Unclassified Information through the Internet unless the Designated Approving Authority has approved the method of transmission in writing.

2. Government office equipment, including Information Technology (IT), shall only be used for official purposes, except as specifically authorized in this Instruction. Employees are permitted limited appropriate use of Government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of Government office equipment should take place during the employee's non-work time. This privilege to use Government office equipment for non-Government purposes may be revoked or limited at any time. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal additional expense to the Government in areas such as:

(a) Communications infrastructure costs; e.g., telecommunications traffic, etc.

(b) Use of consumables in limited amounts; e.g., paper, ink, toner, etc.

(c) General wear and tear on equipment.

(d) Data storage on storage devices.

(e) Transmission impacts with moderate electronic mail (E-mail) message sizes, such as E-mails with attachments smaller then 10 megabytes.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
17 Nov 1999	N/A	-

Title and Subtitle Internet Policy	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 10	

3. This policy in no way limits employee use of Government office equipment, including IT, for official activities.

4. It is the responsibility of employees to ensure that their personal use of Government office equipment is not falsely interpreted to represent the agency. If there is an expectation of such an interpretation, a disclaimer must be used, such as "The contents of this message are mine personally and do not reflect any position of the Government or my agency."

5. Employees do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet or using E-mail. To the extent that employees wish that their private activities remain private, they should avoid using office equipment such as the computer, Internet or E-mail. By using Government office equipment, employees imply their consent to disclosing the contents of any files or information maintained or pass-through Government office equipment. By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using E-mail. Any use of Government IT is made with the understanding that such use is generally not secure, private or anonymous.

6. Employees shall download E-mail attachments and files transferred through the Internet to a floppy diskette whenever possible and check for viruses before they expose OIG computers to this electronic information. If the file is too large to download to a floppy diskette, the employee shall check for viruses before executing the file from the hard disk.

7. Employees shall not send or receive copyrighted graphics or documents through the Internet without the owner's permission.

8. The employee's manager must approve subscriptions to mailing list services. Such subscriptions must be related to an employee's work. Large volumes of E-mail traffic from subscriptions cause delays and other problems for the OIG local area network – wide area network (LAN-WAN). Therefore, they should be kept to a minimum.

9. The OIG reserves the right to monitor all Internet communications for the performance of operation, maintenance, auditing, security or investigative functions. Further, monitoring is used to enforce policies regarding official use and harassment and to access information when an employee is not available. Because the OIG, DoD, is responsible for servicing and protecting its LAN-WAN, authorized employees may monitor or disclose, or assist in monitoring or disclosing, Internet communications. The Chief Information Officer (CIO) must provide authorization for this monitoring.

10. Inappropriate personal use of the Internet, to include use of the Internet or E-mail, could result in loss of use or limitations on use of the Internet, disciplinary or adverse action, criminal penalties and/or the employee being held financially liable for the cost of the improper use.

11. Employees are specifically prohibited from using Government office equipment to maintain or support a personal private business or to assist relatives, friends or other persons in such activities.

F. Responsibilities

1. The **CIO** shall:

a. Approve, for the OIG, DoD, policies implementing laws and guidelines on Internet use.

b. Provide leadership to manage Internet use within the OIG, DoD.

c. Authorize monitoring.

d. Oversee the promulgation of policies and guidance to ensure the most effective and efficient use of Internet resources.

2. **Employees** who use the Internet shall:

a. Read, understand and abide by this policy and its provisions.

b. Access and use the Internet in accordance with established laws, procedures and guidelines. Those include, but are not limited to, references a through l.

c. Refrain from any practices that might jeopardize, compromise or render useless any OIG data, system or network.

d. Be individually responsible and liable for any disclosures of personal information if the employee chooses to send such information through an electronic communications system provided by the OIG, DoD, or Federal Government, or both.

e. Not send secure, sensitive, classified or potentially embarrassing information through an electronic communications system provided by the OIG, DoD, or Federal Government, or both unless approved by the Designated Approving Authority.

f. Refrain from any activities that could congest or disrupt an electronic communications system provided by the OIG, DoD, or Federal Government, or both.

g. Properly disconnect from Internet applications when work has been completed. This will free up and ensure appropriate bandwidth for other employees.

h. Keep files and messages stored on-line to a minimum needed to support current projects or job duties. Perform backup of files and E-mail on a regular basis.

i. Scan any file or message received through the Internet for viruses before running an executable file or opening a document. Newer viruses are embedded within several different types of documents.

j. Refrain from any inappropriate personal uses.

3. **OIG Component Heads** shall:

a. Establish component-level policies for access and use of the Internet to the extent they deem appropriate to accomplish job responsibilities.

b. Ensure that employees are trained properly in accessing and using the Internet.

c. Monitor appropriate access and use of the Internet by employees.

d. Ensure that employees meet the provisions of this Instruction.

4. The **Personnel and Security Directorate, OA&IM,** as the Designated Approving Authority, shall:

a. Assist and advise on the security implications of accessing and using the Internet and its resources.

b. Ensure AIS use complies with applicable security laws, guidelines, regulations and standards, both internal and external.

c. Serve as the Designated Approving Authority.

d. Advise and assist management on appropriate administrative action(s) if misuse occurs.

5. The **Information Systems Directorate, (ISD), OA&IM**, shall:

a. Make Internet service available to OIG, DoD, employees based on justified requirements to access and use the Internet and its resources, as determined by OIG Component Heads.

b. Coordinate the administration of all technical aspects of providing Internet services to the OIG, DoD, through its LAN-WAN.

c. Have technical control of the OIG Internet connection.

d. Monitor the use of electronic communications to ensure adequate performance and proper use, as approved by the CIO.

e. Use or disclose information obtained during the monitoring process only as required in the performance of official duties.

f. Notify the CIO of any problem concerning an employee's conduct in accessing and using the Internet and its resources.

g. Develop and maintain all official OIG, DoD Web Sites and all subsidiary WebPages approved by the CIO.

G. Procedures

1. To receive Internet E-mail, an employee must first establish a personal address. To do so, on the E-mail menu, the employee shall select the "Compose" option. On the "To:" line of the blank E-mail message, the employee shall type:

INET[Dummy@DODIG.OSD.MIL]

2. The system responds with the employee's new Internet address. The employee must provide that address to parties who wish to send messages to the employee through the Internet. No comprehensive on-line directory of Internet addresses exists.

3. For subsequent access, the employee shall select the "Compose" option on the E-mail menu. On the "To:" line of the blank E-mail message, the employee shall type:

INET[Addressee]

4. Employees shall check for viruses that may accompany software downloaded from, and files transferred through, the Internet. Protection from viruses includes downloading the files to diskettes, whenever possible, and scanning before placing files on the hard drive. If employees must

decompress files, they shall perform a second virus check of the decompressed files. If the file or software is too large to download onto a floppy diskette, the employee shall check for viruses before executing or opening the file or software from the hard disk.

5. If the employee introduces any software, including that obtained from the Internet, into the OIG, DoD, environment that the ISD, OA&IM, did not issue, the employee is totally responsible for the software. That includes any effect that it may have on the operation of standard hardware and software as defined in reference g. Even virus-free software may cause conflicts. If the ISD, OA&IM, determines that introduced software is causing a malfunction of standard hardware or software, the ISD, OA&IM, shall return the employee to the standard configuration. The ISD, OA&IM, shall not assume responsibility for any functionality or data lost by returning to standard configuration. The employee is also responsible for operating the software within established laws, guidelines and procedures, including software licensing agreements. In accordance with reference g, any OIG component that chooses to use nonstandard software must manage, maintain and support that software.

6. When the ISD, OA&IM, detects inappropriate use or abuse of the Internet, the ISD, OA&IM, personnel shall provide a detailed hardcopy of the employee's accessed sites to the CIO.

7. If the CIO determines Internet access shall be denied, the CIO shall provide the hard copy logs to the OIG Component Head or his or her designee.

8. If the OIG Component Head requires additional proof, the ISD, OA&IM, shall capture other data and provide the data to the OIG Component Head or his or her designee.

9. The OIG Component Head or his or her designee shall expeditiously pursue any appropriate administrative action.

10. The OIG Component Head or his or her designee shall determine whether the employee's computer hardware and software shall be removed and inform the ISD, OA&IM, to remove the computer hardware and software.

11. When the OIG Component Head or his or her designee determines that the employee's Internet access shall be restored, the OIG Component Head or his or her designee shall provide the ISD, OA&IM, a signed Network Access Request form. The ISD, OA&IM, shall restore LAN-WAN and Internet access and shall return computer hardware and software that has been removed upon receipt of the form.

H. OIG Component Field Activity Guidance on Access to the Internet

1. Any OIG component field activity that does not have access to the OIG WAN must determine the availability of Internet connection through a local Government facility. The OIG component field activity's selection of an Internet Service Provider (ISP) versus the use of a Government facility must clearly be to the advantage of the Government.

2. The OIG component field activity must evaluate the services of local ISPs within its immediate geographic area. The OIG component field activity must compare, at a minimum, the providers' scope of services, fees, prices and level of support. The OIG component field activity must prepare a memorandum for the ISD, OA&IM, and send it through the component's Information Systems Liaison. The memorandum must document the market research of the capabilities of the various ISPs. The memorandum shall include information, such as the ISP's outbound capability (for example, one Analog line versus T-1 lines), backup power, number of incoming lines, etc. The data should be a part of the OIG component field activity's selection criteria for choosing a particular ISP.

3. The OIG component field activity shall fund the costs associated with access to the Internet. The OIG component field activity must determine what type of monthly or yearly fee structure is to the advantage of the Government. The OIG component field activity shall identify anticipated costs to its Information Systems Liaison and the Financial Management Directorate, OA&IM, to ensure that funds are available at the OIG component field activity before contracting for services.

4. The OIG component field activity shall determine, working with an ISP or personnel at the selected Government facility, the minimum hardware and communication requirements necessary to properly access the Internet. The OIG component field activity shall prepare requirements documentation indicating the need for Internet access, market analysis and other documentation. The OIG component field activity shall send the requirements documentation to the component's Information Systems Liaison, along with requirements for a hardware upgrade or any other requirements.

5. Unless it clearly justifies otherwise to the OIG Component Head, the OIG component field activity shall use only one Internet account.

6. A field activity that uses the OIG, DoD, WAN shall use procedures provided by the ISD, OA&IM, personnel.

I. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

APPENDIX A
REFERENCES

a. DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AISs),” March 21, 1988

b. DoD 5500.7-R, “Joint Ethics Regulation (JER),” August 1993, as changed

c. IGDINST 4630.1, Electronic Mail Policy, September 19, 1997

d. IGDINST 5400.7, Inspector General Freedom of Information Act Program, December 16, 1991, as changed

e IGDM 5015.2, Records Management Program, October 25, 1994

f. IGDPH 5200.1, Introduction to Security, June 1993

g. IGDINST 7950.2, Inspector General Microcomputer Hardware and Software Management Program, August 11, 1997

h. DoD 5200.2-R, “Personnel Security Program,” January 1987, as changed

i. DoD 5200.28-M, “ADP Security Manual,” January 1973, as changed

j. DoD Directive 5500.7, “Standards of Conduct,” August 30, 1993, as changed

k. Freedom of Information Act, 5 U.S.C. 552, as amended

l. Privacy Act of 1974, 5 U.S.C. 552a, as amended

APPENDIX B
DEFINITIONS

1. **Chief Information Officer (CIO).** The senior official appointed by the Inspector General, Department of Defense, who is responsible for developing and implementing information resources management in ways that enhance OIG mission performance through the effective, economic acquisition and use of information.

2. **Designated Approving Authority (DAA).** The official designated by the Inspector General, Department of Defense, who has the authority to decide on accepting the security safeguards prescribed for an information system. The DAA issues an accreditation statement that records the decision to accept those standards.

3. **Employee Non-Work Time.** Times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use Government office equipment during off-duty hours, such as before or after a workday (subject to local office hours), lunch periods, authorized breaks or weekends or holidays (if the employee's duty station is normally available at such times).

4. **Inappropriate Personal Uses.** Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of Government office equipment includes, but is not limited to:

a. Any personal use that could cause congestion, delay or disruption of service to any Government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. "Push" technology, such as Pointcast on the Internet, Real Audio and other continuous data streams would also degrade the performance of the entire network and could be considered an inappropriate use.

b. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.

c. The creation, copying, transmission or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter.

d. Using Government office equipment for activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.

e. The creation, downloading, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.

f. The creation, downloading, viewing, storage, copying or transmission of materials related to gambling, weapons, terrorist activities and any other illegal activities or activities otherwise prohibited, etc.

g. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

h. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity or engaging in any prohibited partisan political activity.

i. Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained, or uses at odds with the agency's mission or positions.

j. Any use that could generate more than minimal additional expense to the Government.

k. The unauthorized acquisition, use, reproduction, transmission or distribution of any controlled information, including computer software and data that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data or export controlled software or data.

5. **Information Technology.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.

6. **Internet Service Provider (ISP).** A company that provides subscribers with access to the Internet and on-line services for a fee.

7. **Internet**. The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

8. **Mailing List Service.** An electronic forum or discussion group dedicated to a specific interest or topic and distributed as electronic mail (E-Mail) messages to individual mail boxes. Subscribers automatically receive all E-Mail messages posted to the mailing list service.

9. **Minimal Additional Expense.** Employee's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the Government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include, but are not limited to, making a few photocopies, using a computer printer to print a few pages of material, infrequently sending personal E-mail messages or limited use of the Internet for personal reasons.

10. **Personal Use.** Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Employees are specifically prohibited from using Government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a Government computer and Internet connection to run a travel business or investment service. The ban on using Government office equipment to support a personal private business also includes employees using Government office equipment to assist relatives, friends or other persons in such activities. Employees may, however, make limited use under this policy of Government office equipment to check their Thrift Savings Plan, to seek employment in response to Federal Government downsizing or communicate with a volunteer charity organization.

11. **Privilege.** In the context of this policy, privilege means that the Executive Branch of the Federal Government is extending the opportunity to its employees to use Government property for personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use Government office equipment for non-Government purposes. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes. Government office equipment, including information technology, includes, but is not limited to, personal computers and related peripheral equipment and software, office supplies, Internet connectivity and access to Internet services and E-mail.

12. **Sensitive Unclassified Information.** Any information that has not been specifically authorized to be kept classified, but that if lost, misused, disclosed or destroyed, could adversely affect the national interest or the conduct of OIG operations or Federal programs, or the privacy to which individuals are entitled under the Privacy Act. Typical types of sensitive data are "For Official Use Only," proprietary, financial and mission critical information.

13. **Web Site.** A collection of information organized into a number of Web documents related to a common subject or set of subjects, including the "home page" and the linked subordinate information.